



Department of Homeland Security Daily Open Source Infrastructure Report for 10 July 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- Newsday reports both the New York Police Department and the Port Authority police, who patrol the tunnels and the commuter rail, have stepped up their presence in response to the unfolding plot to blow up train tunnels in the Hudson River. (See item [15](#))
- The Associated Press reports states are lining up ahead of the August 1 deadline to buy Tamiflu and other anti-flu medications from the federal government for a possible pandemic. (See item [28](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *July 08, Denver Post* — **Greenspan raises red flag on energy.** Former Federal Reserve Chairman Alan Greenspan warned Thursday, July 6, that the nation needs to develop alternative energy sources or risk dire economic consequences. Greenspan called for a mixture of solutions, from plug-in hybrid cars to ethanol to nuclear power, to diminish the country's reliance on foreign oil. Greenspan addressed a crowd at the Aspen Institute's Aspen Ideas Festival. Greenspan's comments came a day after oil prices reached a record high, pushing above \$75 a barrel on the New York Mercantile Exchange. His comments largely echoed testimony he made to the Senate Foreign Relations Committee a month ago. In that speech, he

warned that the nation's reliance on foreign oil could have damaging economic consequences because of U.S. reliance on unfriendly nations and vulnerability to terrorists. Greenspan said the nation may also need to develop more nuclear facilities and import more natural gas.

Source: http://www.denverpost.com/business/ci_4021400

2. *July 07, Reuters* — **Oil hits record \$75.78 on strong demand.** Oil hit a fresh record high of \$75.78 a barrel on Friday, July 7, boosted by strong demand in the U.S. and global tension ranging from Iran's nuclear work to North Korea's missile tests. U.S. gasoline demand gained by 1.4 percent in the last four weeks from a year ago, a government report said on Thursday. Adjusted for inflation, oil is more expensive than at any time since 1980, the year after the Iranian revolution. Oil in New York is up 24 percent this year because of supply cuts in Nigeria, the dispute over Iran's nuclear program and a flood of investment fund money into commodities.

Source: http://www.washingtonpost.com/wp-dyn/content/article/2006/07/07/AR2006070700335_pf.html

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

3. *July 09, NewsOK (OK)* — **Ammonia leak forces evacuation.** An ammonia leak forced local officials to evacuate a chicken processing plant in Fairland, OK, on Friday, July 7. Emergency crews blocked a half-mile section of U.S. 59 near the plant and evacuated about 30 homes for a half-hour after the spill.

Source: <http://newsok.com/article/1907907>

4. *July 09, Associated Press* — **Explosion and fire at Idaho plant kills one.** An explosion and fire Friday, July 7, at a building being converted into a biodiesel plant in New Plymouth, ID, killed one man and injured the victim's father and another employee, state police said. Residents who had been temporarily evacuated were allowed to return to their homes on the afternoon of Friday, July 7.

Source: http://www.baytownsun.com/wire.lasso?report=/dynamic/stories/B/BIODIESEL_EXPLOSION?SITE=TXGAL&SECTION=HOME&TEMPLATE=blank.html&CTIME=2006-07-08-00-15-34

5. *July 07, Sun News (SC)* — **Five-truck pile-up on South Carolina bridge spills gas, diesel, snarls traffic.** Five trucks crashed on the "big bridge" on U.S. 17 in North Myrtle Beach, SC on Friday, July 7. Gasoline, diesel and grease spilled across the bridge and shut down the southbound lanes, snarling traffic, officials said. Southbound traffic was at a standstill for more than three hours while northbound traffic crawled through. The Coast Guard arrived on scene to inspect fuel that spilled into the waterway below the bridge, said Brian Williamsen, North Myrtle Beach police spokesman. The South Carolina Department of Health & Environmental Control was also notified, he said.

Source: <http://www.myrtlebeachonline.com/mld/sunnews/14987240.htm>

[[Return to top](#)]

Defense Industrial Base Sector

6. *July 07, Aviation Now* — **Industry association sounds alarm over proposed DoD contracting legislation.** Concerned over the possible ramifications of Senate defense authorization language that would require fixed-price contracts for most Department of Defense (DoD) development programs, the Aerospace Industries Association (AIA) is urging Congress to explore other methods to control costs. Fixed-price government contracts place most of the risk in the lap of the contractor, and are more typically used for technically mature products. Despite its current boom, the defense industry already has the lowest returns of any major manufacturing sector in the U.S., AIA President John Douglass said. A mandate for fixed-price contracting on most development programs could push the industry's margins even lower. As a result, contractors might begin inflating their bids, which would make initial costs go up rather than down, according to Douglass.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/AIA07076.xml

7. *July 06, Government Accountability Office* — **GAO-06-666: Defense Acquisitions: Further Management and Oversight Changes Needed for Efforts to Modernize Cheyenne Mountain Attack Warning Systems (Report).** The Cheyenne Mountain Operations Center houses numerous complex computer systems for tracking air, missile, and space events that could threaten homeland security or undermine military operations in theater. To ensure this mission can be met, the systems require ongoing upgrades. The most recent upgrade program — the Combatant Commanders' Integrated Command and Control System (CCIC2S) — was initiated in 2000. Given the critical missions supported by Cheyenne Mountain systems, the Government Accountability Office (GAO) initiated a review to (1) determine the status of the CCIC2S program in terms of meeting its cost, schedule, and performance goals; (2) gauge the extent to which the Department of Defense (DoD) has followed best practices in managing program requirements; and (3) assess DoD's control and oversight mechanisms for CCIC2S. GAO is recommending that DoD designate CCIC2S as a major acquisition program; establish effective management controls; and conduct an affordability assessment, economic analysis, and independent estimate of life-cycle costs. DoD agreed to designate CCIC2S as a major acquisition program and establish management controls, and stated that it will conduct the affordability assessment and other analyses on future CCIC2S development activities.
Highlights: <http://www.gao.gov/highlights/d066666high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-666>

[[Return to top](#)]

Banking and Finance Sector

8. *July 07, News Sentinel (TN)* — **Hacker enters University of Tennessee data system.** The University of Tennessee (UT) mailed out letters Thursday, July 6, to nearly 36,000 people whose personal information was on a UT computer accessed by a hacker for several months beginning last August. The computer contained the names, addresses, and Social Security numbers of every UT employee and student employee on UT campuses from Knoxville to

Memphis and at every UT office in the state as of last August. It also contained that information for about 4,100 individuals — included among the 36,000 — who received compensation or privileges from UT. UT officials said Thursday there is no indication that whoever got into what would be classified as a small server on UT's Agricultural Campus in Knoxville used any of the information. The hacker was using the computer to store movies for what was apparently an illegal pay movie service on the Internet.

Source: http://www.knoxnews.com/kns/local_news/article/0.1406.KNS_347_4827544,00.html

9. *July 07, Finextra* — **ADP says investor data stolen by scammers.** U.S. investor services and payroll firm Automatic Data Processing (ADP) has admitted that it was tricked into disclosing personal data on thousands of brokerage customers to scammers posing as corporate officers. According to a Reuters report ADP gave shareholder data to "an unauthorized party" who fraudulently requested the data. The data includes names, addresses, and number of shares owned by individual investors, but did not include account numbers or social security numbers and did not identify the brokers where shares were held. Fidelity Investments has reportedly said that around 125,000 of its customers were among those whose data was breached. Around 10,000 UBS customers are thought to be affected along with 3800 Morgan Stanley clients and an undisclosed number of Merrill Lynch clients.

Source: <http://finextra.com/fullstory.asp?id=15544>

10. *July 06, Canadian Broadcasting Corporation* — **Debit-card scam empties Ottawa bank accounts.** Debit-card scamming in Ottawa has reached a new level, with thieves stealing Interac machine keypads from a dozen stores and making withdrawals from hundreds of bank accounts. Thieves trade legitimate controllers for modified units that store PIN information for up to 200 cards. They then take the bank information gathered through the modified keypads and download it to blank debit cards. Since March, the process has led to more than \$2 million in losses for local bank-card users. Police say the scam is likely aided by store workers who look the other way while thieves replace a PIN pad with one modified to steal the banking information from the debit card, along with the PIN.

Source: <http://ca.news.yahoo.com/s/06072006/3/ottawa-debit-card-scam-empties-ottawa-bank-accounts.html>

11. *July 06, Plain Talk (SD)* — **Foiled scams top \$1 million for First National Bank.** First National Bank South Dakota has helped stop \$1,130,397.23 in fraud for its customers so far in 2006. The counterfeit and fraud checks were received by bank customers and either turned in or caught by the alert staff at the bank. The bank's security officer, Lee Gass, said "What we've stopped at the bank so far this year comes from Nigerian scams, Internet sales schemes, fake lottery winnings,' and various other types of fraud..." To keep staff on alert, Gass regularly notifies all staff of reported fraud throughout the U.S. Almost on a daily basis, he relays alerts to the staff about counterfeit bank checks, cashiers checks, and other false monetary exchanges. There can be as many as six of these alerts a day, and some of these strike very close to home.

Source: http://www.plaintalk.net/stories/07062006/localnews_20060706_021.shtml

12. *July 05, Chicago Sun-Times* — **Western Illinois University alumni told of computer breach.** A computer hacker accessed computer systems containing confidential personal data of Western Illinois University alumni a month ago, but some of the more than 180,000 people affected only learned of the problem this week. School spokesperson John Maguire emphasized

that although Social Security numbers and some credit card information were kept in the breached systems, the school has no evidence that any information has been used maliciously. In notices sent beginning June 26, the university told alums and others that the security breach happened June 5. A hacker or hackers accessed "several Electronic Student Services systems," according to information posted on the school's Website. Personal data, names, Social Security numbers, addresses and phone numbers for anyone who took a course at the school since 1983 were kept on the computer system. An additional 1,000 records from students who attended between 1978 to 1982 were also kept on the compromised system. Data from some applicants who did not attend Western might have been accessed. Credit card account numbers for people who bought merchandise through the school's Website or who stayed at the University Union hotel might also have been accessed.

Source: <http://www.suntimes.com/output/news/cst-nws-westernhack05.ht ml>

[[Return to top](#)]

Transportation and Border Security Sector

13. July 09, CNN — Russia airline crash kills 124. A Sibir Airlines passenger jet with 200 people on board veered off the runway early Sunday, July 9, while landing at Irkutsk Airport in eastern Siberia, crashed into a concrete barrier and burst into flames, killing at least 124 people, according to the Russian Ministry of Emergency Situations. The front of the Airbus A-310 was crushed, and 53 people were hospitalized, most of them with burns, the ministry told CNN. The plane was carrying eight crewmembers and 192 passengers at the time of the crash, a Sibir Airlines spokesperson Konstantin Koshman told "Russia Today" English language news service. So far, 120 bodies have been recovered, the ministry said. Another 25 are missing and while most are feared dead, witnesses reported seeing some people jumping from the wreckage and leaving the crash site. The jet, flying from Moscow, hit a building before catching fire, the agency said. Russian Transport Minister Igor Levitin blamed the crash of the Airbus A-310 on wet runway conditions after rain, Russian news agencies reported. CNN's Senior International Correspondent Mathew Chance said that the airline — Russia's second largest — has a good reputation and reports suggested pilot error may have been a factor.

Source: <http://www.cnn.com/2006/WORLD/europe/07/09/russia.crash/index.html>

14. July 08, Chicago Sun-Times — Midway mechanic charged with stealing medical bags. A 30-year-old Crestwood, IL, man was arrested on his first day on the job as a mechanic with Southwest Airlines, during an investigation into employee theft of medical bags on planes, officials said. Anthony J. Donato, who had his court appearance Friday, July 7, is charged with one count of burglary in connection with a June 30 incident aboard a Northwest Airlines plane. Security officers for Northwest allegedly spotted Donato boarding the plane shortly after 1 a.m. CDT with a flashlight and screwdriver, the Cook County State's Attorney's office said. Two officers stationed on the plane stopped Donato after he went into a closet and allegedly removed a medical bag containing bandages, painkillers, and other supplies intended for sick passengers.

Source: http://cbs2chicago.com/topstories/local_story_189113842.html

15. July 08, Newsday (NY) — New York police increase transit presence. The New York Police Department (NYPD) has posted additional officers in lower Manhattan in recent weeks in

response to the unfolding plot to blow up train tunnels in the Hudson River, Commissioner Ray Kelly said. And in a coincidence of timing, still more cops rode the trains Friday, July 7, because of the one-year anniversary of the London subway attacks. Kelly said that both the NYPD and the Port Authority police, who patrol the tunnels and the commuter rail, had stepped up their presence lately in the areas where the plan appears to have been focused. Hercules teams — heavily armed officers that flood a sensitive area at random — have been another crucial element of the city's terror response. Samuel Plumeri, superintendent of the Port Authority police, said his department is focused on protecting the approximately 450 million people who annually use the bridges, tunnels, airports, and trains that the agency oversees. Soon, Jersey City transit riders will be screened for explosives, a measure which Plumeri said was part of a long-term plan and not connected to the latest plot.

Source: <http://www.newsday.com/news/local/newyork/ny-nysecu084810583jul08.0.737133.story?coll=ny-nycnews-headlines>

16. *July 07, Government Accountability Office* — GAO-06-940T: Border Security:

Investigators Transported Radioactive Sources Across Our Nation's Borders at Two Locations (Testimony). This testimony was given before the Subcommittee on International Terrorism and Nonproliferation, House Committee on International Relations, in Laredo, TX. Given today's unprecedented terrorism threat environment and the resulting widespread congressional and public interest in the security of our nation's borders, GAO conducted an investigation testing whether radioactive sources could be smuggled across U.S. borders. Most travelers enter the United States through the nation's 154 land border ports of entry. Department of Homeland Security U.S. Customs and Border Protection (CBP) inspectors at ports of entry are responsible for the primary inspection of travelers to determine their admissibility into the United States and to enforce laws related to preventing the entry of contraband, such as drugs and weapons of mass destruction. The Government Accountability Office's (GAO) testimony provides the results of undercover tests made by its investigators to determine whether monitors at U.S. ports of entry detect radioactive sources in vehicles attempting to enter the United States. GAO also provides observations regarding the procedures that CBP inspectors followed during its investigation. GAO has also issued a report on the results of this investigation (GAO-06-545R).

Highlights: <http://www.gao.gov/highlights/d06940thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-940T>

17. *July 07, CNN* — Three held in New York tunnel plot. Three of eight "principal players" in an alleged plot to blow up a tunnel between New York City and New Jersey are in custody, the FBI said Friday, July 7. FBI Assistant Director Mark Mershon said the plan was "what we believe was the real deal," a scheme involving al Qaeda members on three continents. Without naming a specific tunnel, Mershon said the target was one of the PATH (Port Authority Trans-Hudson) tubes under the Hudson River connecting New Jersey and Manhattan. The only suspect formally charged is a 31-year-old Lebanese man who has confessed to being the ringleader and has claimed to be an al Qaeda member loyal to Osama bin Laden, Mershon said. The scheme was in the planning stages but was about to move into the execution phase with an attack set for October or November, Mershon said. Nearly two million vehicles pass through New York's tunnels and bridges daily, according to a 2002 estimate by the city's Department of Transportation. Investigators began moving in on the plotters because they were suspected of starting to act, including the surveillance of the target and the collection of materials for the

attack, Mershon said.

Source: <http://www.cnn.com/2006/US/07/07/tunnel.plot/index.html>

18. *July 07, Reuters* — **Major U.S. airlines seeing full planes this summer.** Planes operated by major U.S. airlines are fuller than ever this summer, and the embattled carriers are seeing stronger revenues as a result, analysts said Wednesday, July 5. The record-high load factors bode well for airlines if they can keep the number of empty seats to a minimum. The industry has been weakened by high fuel prices and competitive pressures that make it hard for carriers to keep ticket prices high enough to cover costs. Recent cuts in capacity have also enabled airlines to raise fares to bolster revenue. UAL, parent of United Airlines, said on Wednesday that its passenger load factor reached a record 88.3 percent in June. "We're now seeing the effects of major cuts in flight schedules, and the flights are becoming like sardine cans..." said Joe Schwieterman, a transportation expert at DePaul University. He warned, however, that while demand for airline tickets remains strong, crowded planes could mean long lines and waning customer service. These conditions may blur the distinction between major airlines that cater to business travelers and low-cost carriers that offer cheap, no-frills transportation.

Source: http://www.usatoday.com/travel/flights/2006-07-06-full-plane_s_x.htm

19. *July 07, Department of Homeland Security* — **Securing the nation's rail systems.** Since the terrorist attacks of September 11, 2001, the 7/7 London subway bombings, and the Madrid rail bombings, the Department of Homeland Security (DHS) has taken several steps to manage risk and strengthen our nation's rail and transit systems by: (1) Providing funding to state and local partners; (2) Training and deploying manpower and assets for high risk areas; (3) Developing and testing new technologies, and; (4) Performing security assessments of systems across the country. While the majority of mass transit systems in this country are owned and operated by state and local government and private industry, securing these systems is a shared responsibility between federal, state, and local partners. Since 9/11 the Administration has provided significant resources to bolster these security efforts. Funds from DHS grants programs may be used for planning, training, equipment, and other security enhancements. DHS has provided roughly \$18 billion in awards to state and local governments for programs and equipment that help to manage risk.

Source: <http://www.dhs.gov/dhspublic/display?content=5727>

20. *July 07, Department of Homeland Security* — **Lebanese-U.S. Government disrupt plan to New York-New Jersey transportation system.** The Department of Homeland Security has announced, "Working closely with the Intelligence/Information Directorate within the Internal Security Forces of Lebanon and with other foreign law enforcement and intelligence partners, we have disrupted a terrorist network that was in the planning stages of an attack against the transportation system in the New York-New Jersey area. A significant development in this investigation was the arrest of a key suspect by Lebanese authorities. This investigation is ongoing. We know al Qaeda continues to have an interest in attacking the United States. At this point in time, there is no specific or credible information that al Qaeda is planning an attack on U.S. soil. At the same time, the FBI, through the New York Joint Terrorism Task Force, will continue to investigate suspected activities here and abroad with our partners from the U.S. and international law enforcement and intelligence community. At the same time, the Department of Homeland Security will continue to share information with state and local partners to ensure that they have the appropriate awareness to make decisions about how to best protect their

communities.”

Source: <http://www.dhs.gov/dhspublic/display?content=5726>

21. *July 07, Associated Press* — **Soldier detained for disrupting flight.** A U.S. Army soldier who had served in Iraq was tackled by airplane passengers after he ran down the aisle and rammed the cockpit door on a flight from New York to Tampa on Thursday night, July 6. The soldier did not have any weapons and there was no evidence that he meant harm anyone on the flight, said Tampa International Airport spokesperson Brenda Geoghagan. She said he was restrained until the flight landed and then taken into custody. The soldier's brother told officials that he "has some mental problems related to his Army service," Geoghagan said.

Source: http://www.kare11.com/news/national/national_article.aspx?storyid=128846

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

22. *July 09, Alamogordo Daily News (New Mexico)* — **Three deer test positive for chronic wasting disease.** Three deer in southern New Mexico have tested positive for chronic wasting disease (CWD). The New Mexico Department of Fish and Game received results Wednesday, July 5, from the state Veterinary Diagnostic Services that two wild deer captured near White Sands Missile Range headquarters, and a third wild deer captured near Timburon, tested positive for the disease. To date, the disease has been confined to the southern Sacramento Mountains and areas surrounding the Organ Mountains. Two wild elk from the Sacramentos tested positive in December 2005. The three recent cases bring to 15 the number of infected deer found in the state, since the first case was discovered in 2002.

CWD information: <http://www.cwd-info.org/>

Source: http://www.alamogordonews.com/news/ci_4029107

23. *July 08, Arkansas Democrat* — **Cattle-tracing program under way.** Arkansas Agriculture Secretary Richard Bell reaffirmed the state's commitment to an animal identification program Friday, July 7, during a meeting of the Arkansas Cattlemen's Association. Bell said the department has started the quality systems assessment program for the state's cattle producers. Arkansas will be the second state to have the program, Bell said. Missouri became the first state to develop a voluntary program that identifies the source and age of its cattle in October. The claims are verified by the U. S. Department of Agriculture. Arkansas supplies the beef industry with mostly feeder cattle that are processed in other states. The state has about 1.9 million head of cattle.

Source: <http://www.nwanews.com/adg/Business/159911/>

[\[Return to top\]](#)

Food Sector

Nothing to report.

[[Return to top](#)]

Water Sector

24. *July 09, New York Times* — **E. Coli found in water tests on Fire Island.** Residents and merchants on New York's Fire Island were busy Saturday, July 8, trying to avoid having their weekend spoiled by the threat of E. coli bacteria. Routine sampling of the water mains that serve the island showed signs of the bacteria on Friday, July 7. Officials of the Suffolk County Water Authority were advising residents and restaurant owners to boil water for at least one minute before drinking it or using it to prepare meals. The authorities were expecting to distribute more than 100,000 pounds of bottled water. Michael Stevenson, the water authority's deputy chief executive officer for administration, said that the cause of the positive readings probably was not the actual presence of E. coli in the water supply, but rather a sampling error. He said that the lab results showed the bacteria in several separate pressure zones, and that it was unlikely that the bacteria would travel over such a widespread area.
Source: <http://www.nytimes.com/2006/07/09/nyregion/09ecoli.html>
25. *July 06, U.S. Environmental Protection Agency* — **Nogales, Arizona, fined for safe drinking water violations.** The U.S. Environmental Protection Agency (EPA) recently resolved the city of Nogales, AZ's long-standing drinking water violations regarding its failure to comply with a March 2004 EPA administrative order requiring submittal of drinking water monitoring and reporting data. The city of Nogales will pay a \$5,500 fine and spend at least \$50,000 to repair or replace sewer lines in an area of Nogales commonly referred to as the "old city," where sewer lines have degraded and are leaking wastewater into the surrounding soil and possibly into groundwater supplies. The city failed to meet a March EPA 2005 deadline requiring the municipality to monitor and report chemicals detected in its drinking water. The Nogales system, which provides drinking water to over 19,000 customers, is required to monitor for a number of unregulated contaminants in addition to those regulated by the Safe Drinking Water Act and report the results to the EPA.
Source: <http://yosemite.epa.gov/opa/admpress.nsf/27166bca9a9490ee852570180055e350/ca7441174f652d08852571a3006531ec!OpenDocument>
26. *July 06, U.S. Environmental Protection Agency* — **Revised rule proposed for lead in drinking water.** The U.S. Environmental Protection Agency (EPA) plans to tighten its rules on lead. The proposal would revise monitoring requirements to ensure that water samples show how effective lead controls are; clarify the timing of sample collection and tighten criteria for reducing the frequency of monitoring; require that utilities receive state approval of treatment changes so that states can provide direction or require additional monitoring; require that water utilities notify occupants of the results of any testing that occurs within a home or facility; and require systems to reevaluate lead service lines that may have previously been identified as low risk after any major treatment changes that could affect corrosion control.
More information: <http://www.epa.gov/safewater/lead/>
Source: <http://yosemite.epa.gov/opa/admpress.nsf/27166bca9a9490ee852570180055e350/ca7441174f652d08852571a3006531ec!OpenDocument>

[[Return to top](#)]

Public Health Sector

27. *July 08, Los Angeles Times* — **Bird flu virus reported in Spain for first time.** Spain has recorded its first case of H5N1 bird flu, the Agriculture Ministry said Friday, July 7. The deadly strain was found in a water fowl in a marsh area outside the northern city of Vitoria. A protective area of two miles was declared around the area where the bird was found. Outdoor poultry farming had been banned within six miles of marshlands where migratory birds tend to gather.

Source: <http://www.latimes.com/news/nationworld/nation/la-sci-briefs8.3jul08.1.5414486.story?coll=la-headlines-nation>

28. *July 07, Associated Press* — **States line up for anti-flu medication.** South Carolina is in. Utah and Alabama, too. Some states aren't waiting for an August 1 deadline to seek help from the federal government in buying anti-flu medicine for a possible pandemic. The federal government is stockpiling Tamiflu and other anti-flu medications. The Bush administration plans to buy enough to treat 44 million people. States can buy more if they want. The government is negotiating a price with Roche Laboratories, Inc., which makes Tamiflu, and will pay a quarter of the costs, up to a prescribed amount for each state. In all, states could use the subsidy to buy anti-flu medications for an additional 31 million people. Washington says they plan to take full advantage of the next few weeks to determine the right amount of drugs to purchase. Oklahoma has allocated enough to buy medicine to treat about 35,000 of the state's 3.5 million people. But that's about seven percent of the amount the state could purchase through the federal subsidy. Montana, population 918,000, plans to buy enough anti-flu medication to treat 8,100 people. Arizona has plans to spend one million dollars on 70,000 courses of the 585,780 available to Arizona. New Hampshire said it intends to purchase all the drugs that the federal government is making available to the state.

Source: <http://www.foxnews.com/wires/2006Jul07/0.4670.PandemicStates.00.html>

29. *July 07, Agence France-Presse* — **Indonesian girl dies of bird flu.** A three-year-old Indonesian girl who has died was infected with bird flu, according to local test results, a health ministry official has said. If the results are confirmed by the World Health Organization (WHO), the girl would be the 41st bird flu death in Indonesia, which is close to registering the world's highest number of deaths from the H5N1 virus. Runizar Roesin, a doctor at the health ministry's bird flu center, said the girl died on Thursday, July 6, at a Jakarta hospital.

Source: http://news.yahoo.com/s/afp/20060707/hl_afp/healthfluindonesia_060707102503;_ylt=Am7vkvMrUDaimtM_4LXfUmGJOrgF:_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--

[[Return to top](#)]

Government Sector

30. *May 31, Government Accountability Office* — **GAO-06-612: Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts (Report)**. The protection of U.S. federal facilities has become an important concern due to the ongoing threat of terrorism. The General Services Administration (GSA), U.S. Postal Service (USPS), and the Departments of Veterans Affairs (VA) and Interior (Interior) hold the most domestic, nonmilitary property. Additionally, the Department of Homeland Security (DHS) is responsible for the protection of GSA facilities. DHS chairs the Interagency Security Committee (ISC), which is tasked with coordinating federal agencies' facility protection efforts. The need to better protect federal facilities, as well as federal budget constraints, have prompted the need for these agencies to measure the performance of their facility protection efforts. The Government Accountability Office's (GAO) objectives were (1) to identify examples of performance measures for facility protection being used by selected organizations outside of the federal government; and (2) to determine the status of U.S. federal agencies' efforts to develop and use performance measures as a part of their facility protection programs. GAO is recommending that the Secretary of DHS direct ISC to establish guidance and standards for measuring performance in federal government facility protection. DHS agreed with the findings and recommendations in this report.
Highlights: <http://www.gao.gov/highlights/d06612high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-612>

[\[Return to top\]](#)

Emergency Services Sector

Nothing to report.

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

31. *July 07, Secunia* — **WebEx Downloader plug-in multiple vulnerabilities**. Some vulnerabilities have been reported in WebEx Downloader plug-in, which can be exploited to compromise a user's system. An error exists in the ActiveX and Java versions of the WebEx Downloader plug-in where the source of downloaded components is not properly verified. This can be exploited to install malicious components on a user's system. Hosting Controller contains an error that allows an authenticated user to escalate privileges. Attackers can exploit this issue to gain web administrative privileges. Also, some unspecified boundary errors in an included ActiveX control can be exploited to cause a buffer overflow.
Vulnerable products: WebEx Downloader plug-in 2.x
Solution: Apply update. <http://www.webex.com/go/downloadSP30>
Source: <http://secunia.com/advisories/20956/>
32. *July 06, Security Focus* — **Microsoft Internet Explorer structured graphics control denial-of-service vulnerability**. Microsoft Internet Explorer is prone to a denial-of-service vulnerability. The flaw was discovered after ActiveX fails. This issue is triggered when an attacker convinces a victim user to activate a malicious ActiveX control. Remote attackers may exploit this issue to crash Internet Explorer, effectively denying service to legitimate users.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/18855/info>
Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.
Source: <http://www.securityfocus.com/bid/18855/references>

33. *July 06*, — **New Mac OS feature raises privacy concerns.** Some Apple users are wondering if their privacy is being compromised after installing an updated version of the company's Mac OS X —Version 10.4.7 —that aims to help authenticate desktop widgets. Apple's Dashboard Advisory, another security feature in the recent update, was designed to ensure that the widgets users download are legitimate and authorized by the company that created them. The debate about Mac OS comes at a sensitive time as IT vendors' efforts to track online computing activity, particularly without giving warnings, are raising users' ire and triggering legal action. John Pescatore, an analyst with market research firm Gartner, said these types of issues come at a time when there is a growing debate about balancing end users' security and privacy concerns. Pescatore said the best option for software companies is to ensure that they clearly explain every feature to customers and offer people the option to opt out. "If you sneak it in, it's automatically wrong," Pescatore said on July 6.

Source: <http://www.eweek.com/article2/0.1895.1985712.00.asp>

34. *July 06, Thomson Dialog NewsEdge* — **Scot held by police in computer virus probe.** A Scot has been arrested in connection with a group that infected thousands of computers worldwide with a virus. Matthew Anderson, 28, was picked up by police in Great Britain on Tuesday, July 4. The viruses, attached to "spam" e-mails, run in the background of programs without the owner's knowledge. Once installed, the viruses give criminals access to private information on the computer.

Source: <http://www.tmcnet.com/usubmit/2006/07/06/1706227.htm>

35. *July 06, IDG News Service* — **Microsoft Office 2007 to support ODF standard.** On Wednesday, July 5, Microsoft announced the creation of the Open XML Translator project, so its Office suite will support the OpenDocument Format (ODF) standard. The move comes in response to government requests for Microsoft products to be compatible with ODF, such as the national governments of Belgium and Denmark, and the state government of Massachusetts. The company said that the next edition of Office will include menu options for XML, ODF, and Adobe Systems' PDF formats. A prototype of the first translator for Word's 2007 version was posted Wednesday, July 5, on SourceForge.net, a popular Website for open-source development.

Source: <http://www.pcworld.com/news/article/0.aid.126331.00.asp>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is aware of multiple

vulnerabilities in Microsoft Internet Explorer (IE) 6.0. US-CERT is also aware of a public blog that will be posting new web browser bugs on a daily basis in July. US-CERT will be analyzing relevant vulnerabilities, as well as actively monitoring the site to provide additional information as it becomes available. Please review URL: <http://metasploit.blogspot.com/2006/07/month-of-browser-bugs.html>

Until an update, patch, or more information becomes available, US-CERT strongly recommends the following:

Disable ActiveX

Securing Your Web Browser:

http://www.us-cert.gov/reading_room/securing_browser/#Internet Explorer

Malicious Web Scripts FAQ:

http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

Do not follow unsolicited links.

Review the steps described in Microsoft's document to improve the safety of your browser: http://www.microsoft.com/athome/security/online/browsing_safety.mspx

US-CERT will continue to update current activity as more information becomes available.

Public Exploit Code for Unpatched Vulnerabilities in Microsoft Internet Explorer

US-CERT is aware of publicly available exploit code for two unpatched vulnerabilities in Microsoft Internet Explorer. By persuading a user to double click a file accessible through WebDAV or SMB, a remote attacker may be able to execute arbitrary code with the privileges of the user. US-CERT is tracking the first vulnerability as VU#655100: <http://www.kb.cert.org/vuls/id/655100>

The second issue is a cross domain violation vulnerability that is being tracked as VU#883108: <http://www.kb.cert.org/vuls/id/883108>

Until an update, patch, or more information becomes available, US-CERT recommends the following:

Do not follow unsolicited links.

To address the cross domain violation vulnerability (VU#883108):

<http://www.kb.cert.org/vuls/id/883108>

Disable ActiveX as specified in the Securing Your Web Browser:

http://www.us-cert.gov/reading_room/securing_browser/#Internet Explorer

Review Malicious Web Scripts FAQ:

http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

US-CERT will continue to update current activity as more information becomes available

PHISHING SCAMS

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

http://www.us-cert.gov/nav/report_phishing.html

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 25 (smtp), 445 (microsoft-ds), 6346 (gnutella-svc), 24232 (----), 6881 (bittorrent), 6588 (AnalogX), 32790 (----), 4989 (----), 80 (www) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.